LA BLOCKCHAIN : INTRODUCTION A LA BLOCKCHAIN

Christophe Ozcan

ESME sudria
PARIS | BORDEAUX | LILLE | LYON

christophe.ozcan@esme.fr

PARTIE I
-
GENESE DE LA TECHNOLOGIE BLOCKCHAIN

Le contexte historique
Il était une fois Bitcoin
La signature éléctronique
Réalisation d'une transaction dans un système traditionnel/actuel
Avantages apportés par bitcoin
La communauté open source

L'histoire de la monnaie fiduciaire

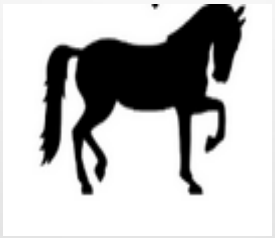
De l'antiquité au 19ème siècle

TROC

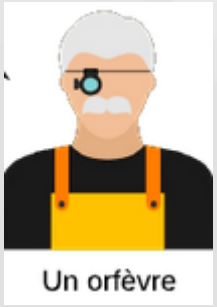
OR

L'histoire de la monnaie fiduciaire

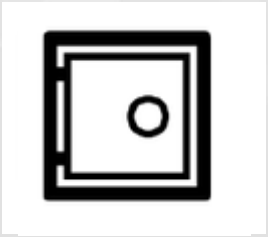
Je t'échange ton cheval contre mon bon d'1kg d'or.

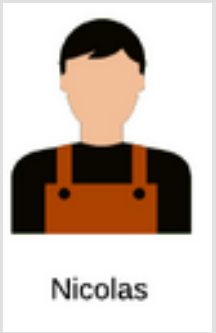


Transfert à un tiers de confiance



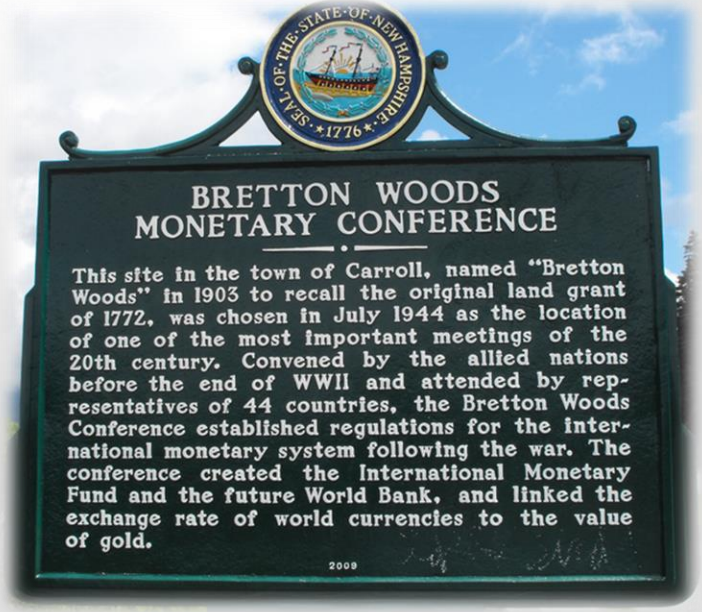
Très bien, voici vôtre or.





Je viens récupérer mes 1kg d'or.

L'histoire de la monnaie fiduciaire



Création du Fond Monétaire International

Le dollar est devenu la valeur de change étalon des Devises nationales.

L'histoire de la monnaie fiduciaire

Un système monétaire basée sur la confiance ?

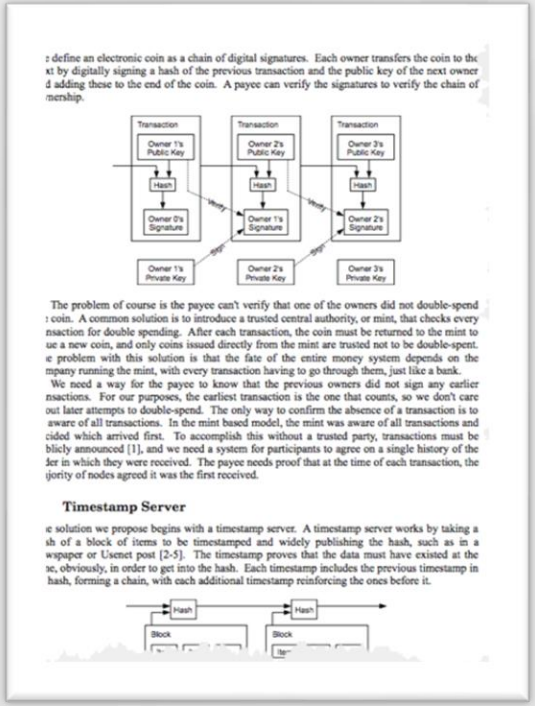
- La crise mondiale des subprimes en 2008
- La crise de la dette publique des états membres de l'union Européenne (Grèce, Portugal, Espagne ..) à partir de 2010
- Dévaluation des devises Asiatique (Chine 3x)

Il était une fois bitcoin

SATOSHI
NAKAMOTO

Bitcoin le père de la technologie Blockchain :

- Publication en 2008 du livre Blanc : *"Bitcoin A Peer-to-Peer Electronic Cash System" par Satoshi Nakamato*



define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the
xt by digitally signing a hash of the previous transaction and the public key of the next owner
d adding these to the end of the coin. A payee can verify the signatures to verify the chain of
nership.

The problem of course is the payee can't verify that one of the owners did not double-spend
coin. A common solution is to introduce a trusted central authority, or mint, that checks every
nsaction for double spending. After each transaction, the coin must be returned to the mint to
ue a new coin, and only coins issued directly from the mint are trusted not to be double-spent.
e problem with this solution is that the fate of the entire money system depends on the
mpany running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier
nsactions. For our purposes, the earliest transaction is the one that counts, so we don't care
out later attempts to double-spend. The only way to confirm the absence of a transaction is to
aware of all transactions. In the mint based model, the mint was aware of all transactions and
cided which arrived first. To accomplish this without a trusted party, transactions must be
blicly announced [1], and we need a system for participants to agree on a single history of the
der in which they were received. The payee needs proof that at the time of each transaction, the
jority of nodes agreed it was the first received.

Timestamp Server

e solution we propose begins with a timestamp server. A timestamp server works by taking a
sh of a block of items to be timestamped and widely publishing the hash, such as in a
wspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the
e, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in
hash, forming a chain, with each additional timestamp reinforcing the ones before it.

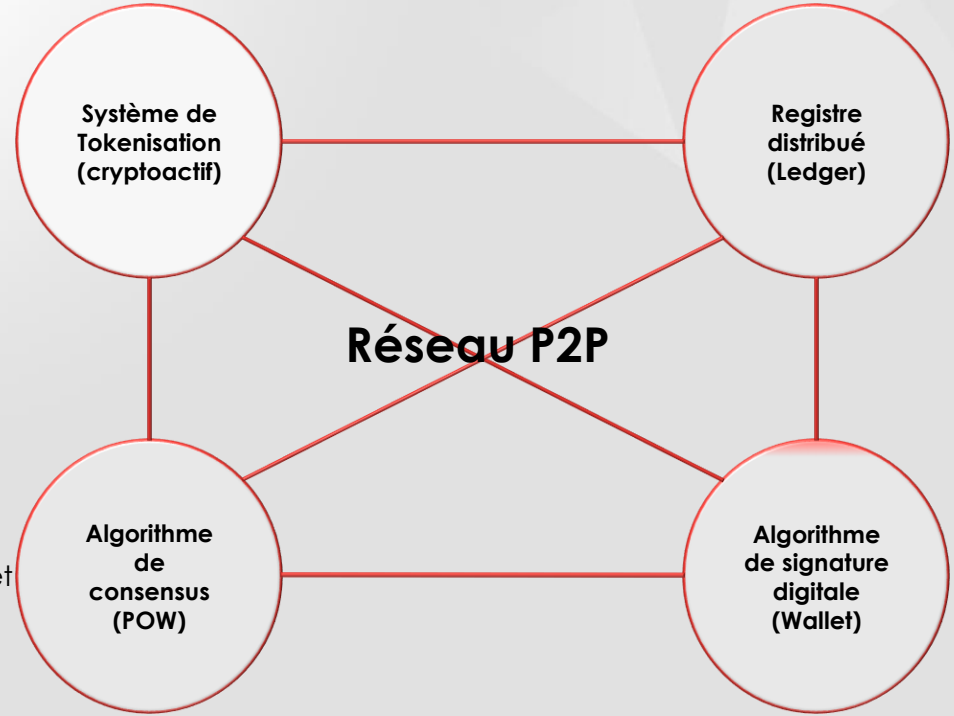
Il était une fois bitcoin

- Description :

“ Bitcoin is an experimental digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: managing transactions and issuing money are carried out collectively by the network.”

- Plus de nécessité de passer par une entité centrale de validation et d’émission de devise
- Toutes les transactions sont publiques et échangées sur un réseau pair à pair décentralisé
- Le nombre de bitcoin en circulation est limité à 21 millions (rareté)
- Logiciel open source publié en 2009 (License MIT : https://github.com/bitcoin)

Nombres : 21 millions de bitcoin (divisible 0.0000001)
Fonction : Réaliser une transaction unique par l'émission de jetons



Fonction : Stocker la chaine de Blocs de transactions

Fonction : Rémunérer les mineurs pour la construction et la validation de Blocs de transactions

Fonction : Authentifier, signer et vérifier électroniquement une transaction

Qu'est ce qu'un algorithme de signature digitale ?

A. Une fonction de génération de clés permettant l'affectation d'un identifiant numérique pouvant être symétrique (une seule clé) ou asymétrique (paire de clé publique/privée)

B. Une fonction de signature pour signer un message ou un contenu

C. Une fonction de vérification pour s'assurer de l'authenticité du message ou du contenu signé par son auteur.

Quelle sont les propriétés de l'algorithme de signature digitale ?

1. **Confidentialité**

Le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé

2. **Authenticité**

Le fait de s'assurer que l'expéditeur est bien celui qu'il prétend être

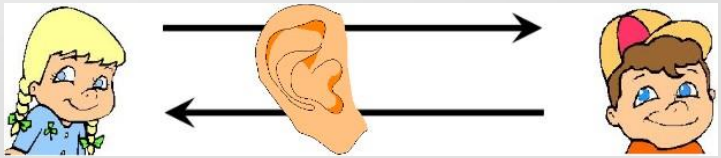
3. **Intégrité**

Le fait de s'assurer que l'information ne subisse aucune altération ou destruction volontaire ou accidentelle, et conserve le format initial

Quelle sont les propriétés de l'algorithme de signature digitale ?

1. **Confidentialité**

Le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé



Contexte

S'assurer du caractère secret de l'information

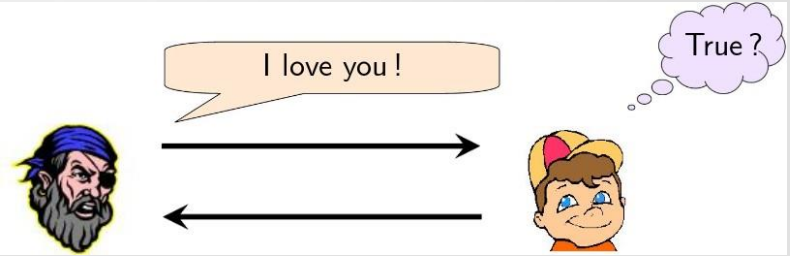
Echange de messages en présence d'un espion

Stockage de données sécurisé

Quelle sont les propriétés de l'algorithme de signature digitale ?

2. **Authenticité**

Le fait de s'assurer que l'expéditeur est bien celui qu'il prétend être



Contexte

S'assurer de la provenance d'un message et de l'authenticité de son émetteur

Quelle sont les propriétés de l'algorithme de signature digitale ?

3. **Intégrité**

Le fait de s'assurer que l'information ne subisse aucune altération ou destruction volontaire ou accidentelle, et conserve le format initial

Contexte

S'assurer de la non-modification d'un message

Qu'est ce qu'un algorithme de signature digitale ?

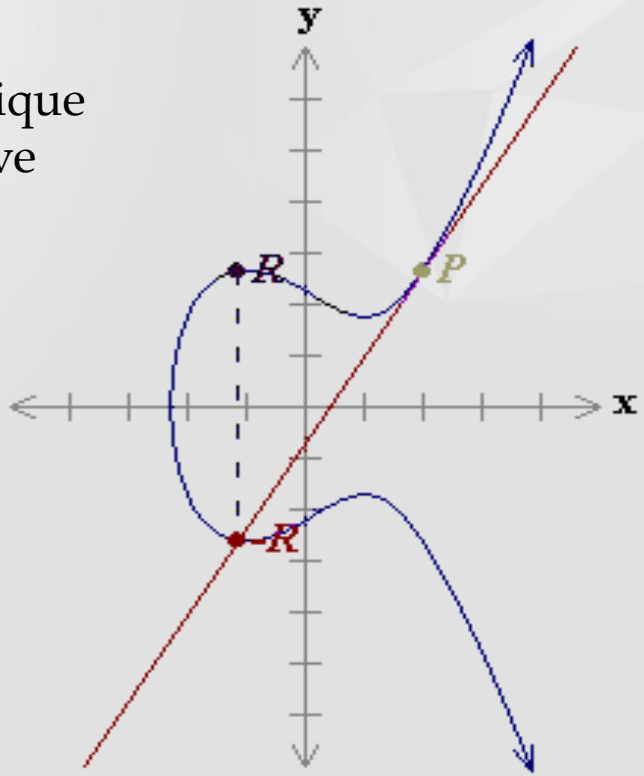
Une **fonction de hachage cryptographique** correspond à une fonction mathématique qui va calculer une empreinte numérique unique de la valeur envoyée sous la forme d'une suite alphanumérique de longueur fixe unique.

Pour cette raison, on dit d'une telle fonction qu'elle est *à sens unique soit non réversible.*

Utilisation de la cryptographie pour la génération de portefeuille :

- Génération du portefeuille électronique

Algorithme de signature numérique « ECDSA* » avec secp256k1 curve



P (2, 2.65)

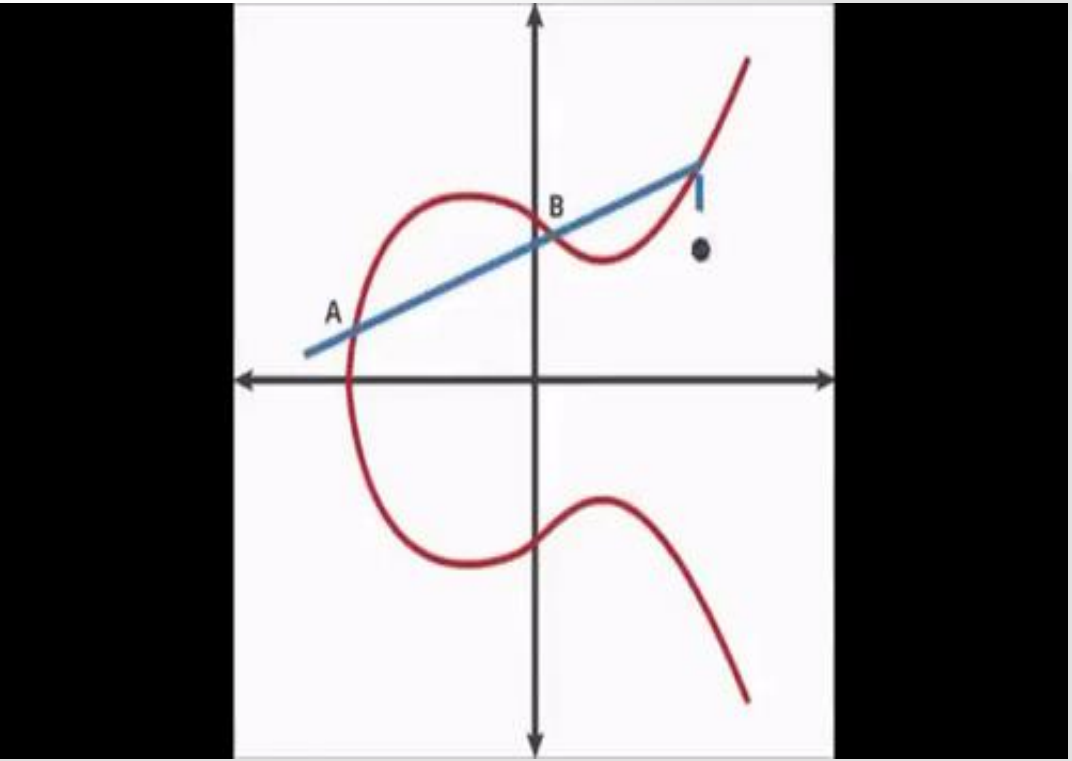
$-R$ (-1.11, -2.64)

R (-1.11, 2.64)

$2P = R = (-1.11, 2.64).$

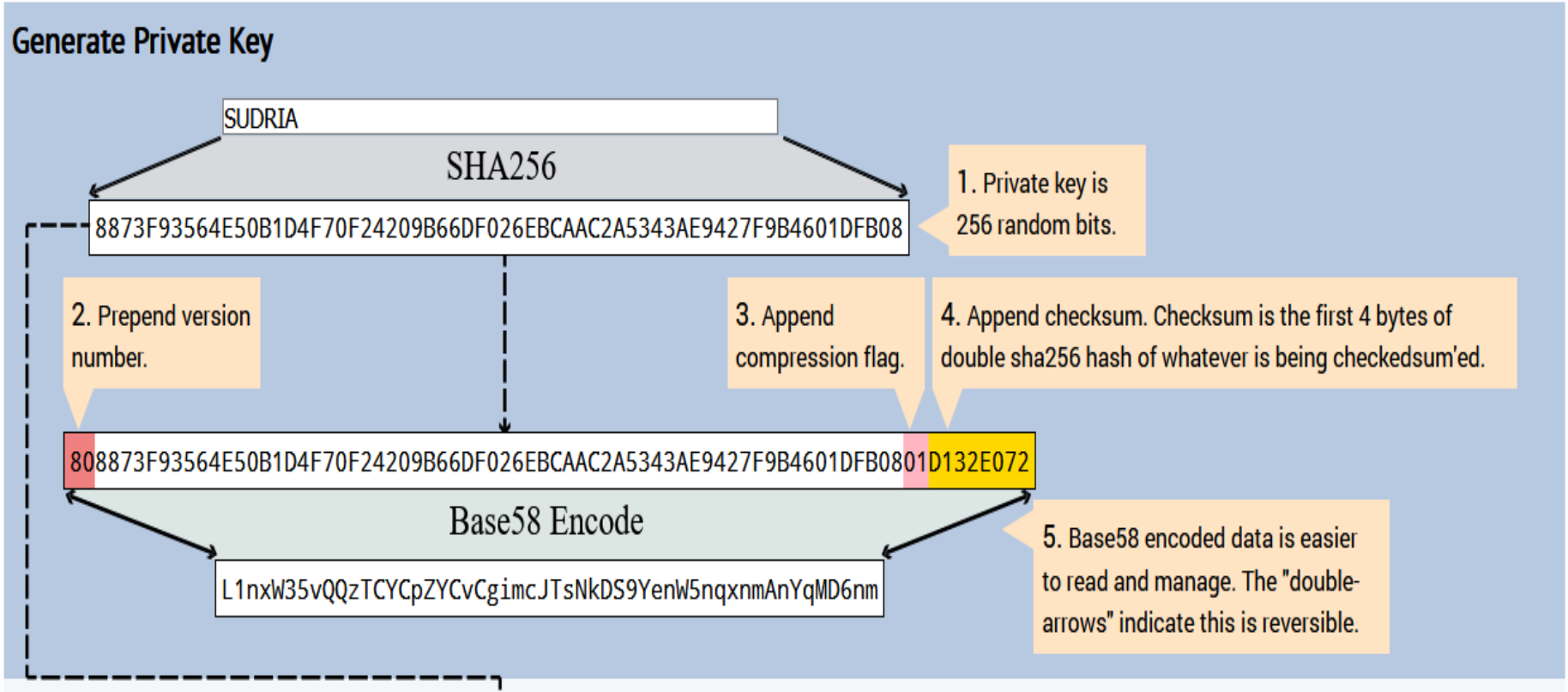
$y^2 = x^3 - 3x + 5$

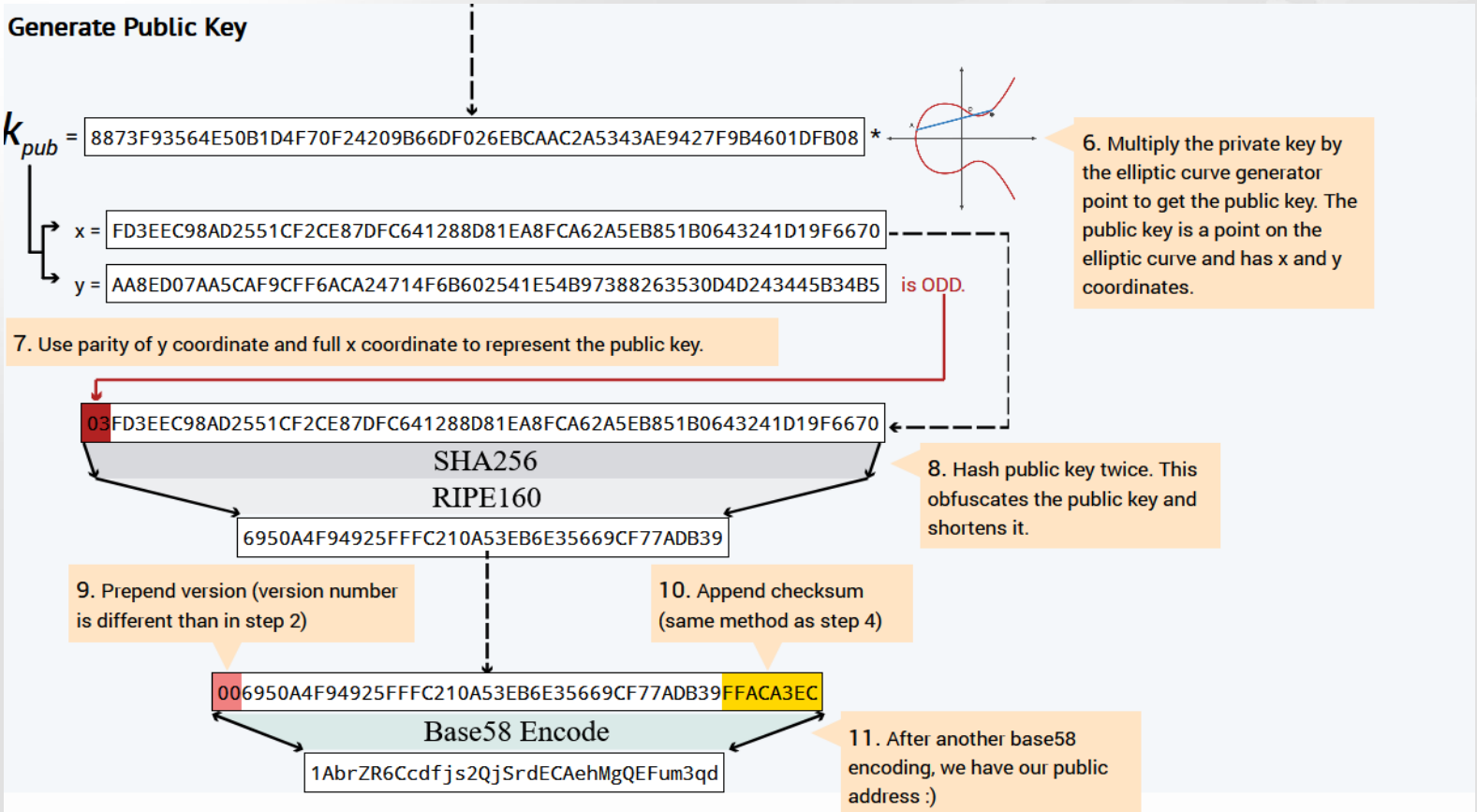
*Elliptic curve digital signature algorithm



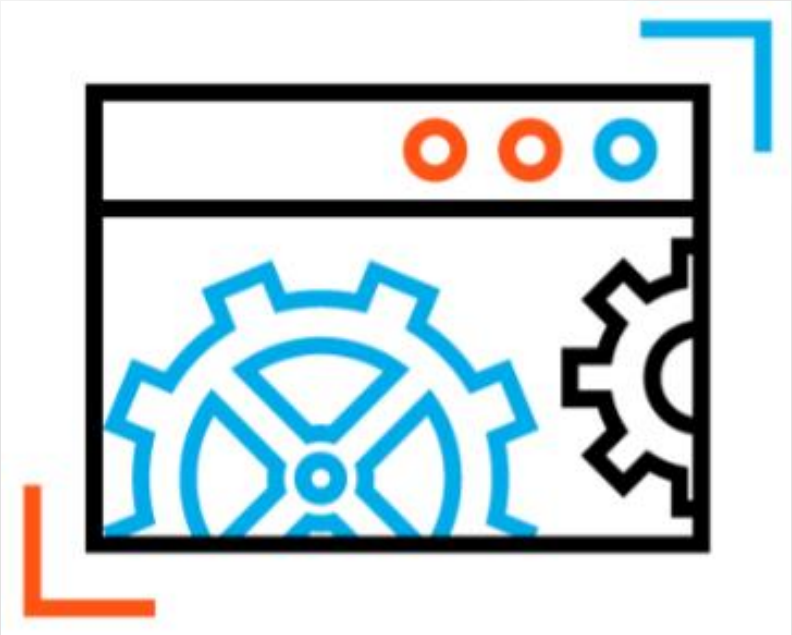
nA = E

n : Randomness number
A : Public key value
E : Private key value


Generate Private Key
SUDRIA
SHA256
8873F93564E50B1D4F70F24209B66DF026EBCAAC2A5343AE9427F9B4601DFB08
1. Private key is 256 random bits.
2. Prepend version number.
3. Append compression flag.
4. Append checksum. Checksum is the first 4 bytes of double sha256 hash of whatever is being checkedsum'ed.
808873F93564E50B1D4F70F24209B66DF026EBCAAC2A5343AE9427F9B4601DFB0801D132E072
Base58 Encode
L1nxW35vQQzTCYCpZYCvCgimcJTsNkDS9YenW5nqxnmAnYqMD6nm
5. Base58 encoded data is easier to read and manage. The "double-arrows" indicate this is reversible.

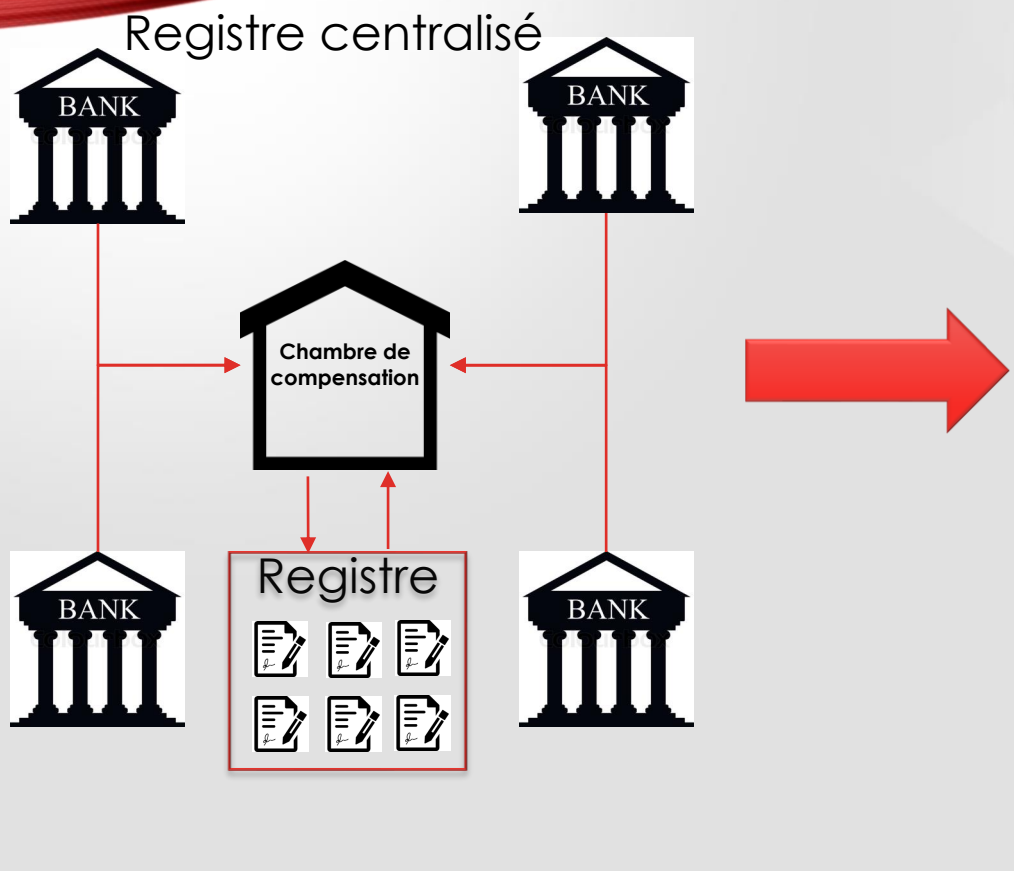

Generate Public Key
k_{pub} = 8873F93564E50B1D4F70F24209B66DF026EBCAAC2A5343AE9427F9B4601DFB08 *
6. Multiply the private key by the elliptic curve generator point to get the public key. The public key is a point on the elliptic curve and has x and y coordinates.
x = FD3EEC98AD2551CF2CE87DFC641288D81EA8FCA62A5EB851B0643241D19F6670
y = AA8ED07AA5CAF9CFF6ACA24714F6B602541E54B97388263530D4D243445B34B5
is ODD.
7. Use parity of y coordinate and full x coordinate to represent the public key.
03FD3EEC98AD2551CF2CE87DFC641288D81EA8FCA62A5EB851B0643241D19F6670
SHA256
RIPE160
8. Hash public key twice. This obfuscates the public key and shortens it.
6950A4F94925FFFC210A53EB6E35669CF77ADB39
9. Prepend version (version number is different than in step 2)
10. Append checksum (same method as step 4)
006950A4F94925FFFC210A53EB6E35669CF77ADB39FFACA3EC
Base58 Encode
11. After another base58 encoding, we have our public address :)
1AbrZR6Ccdfjs2QjSrdECAehMgQEFum3qd

Démonstration Génération de Wallet



CARACTERISTIQUES DE LA TECHNOLOGIE BLOCKCHAIN

Le registre distribué

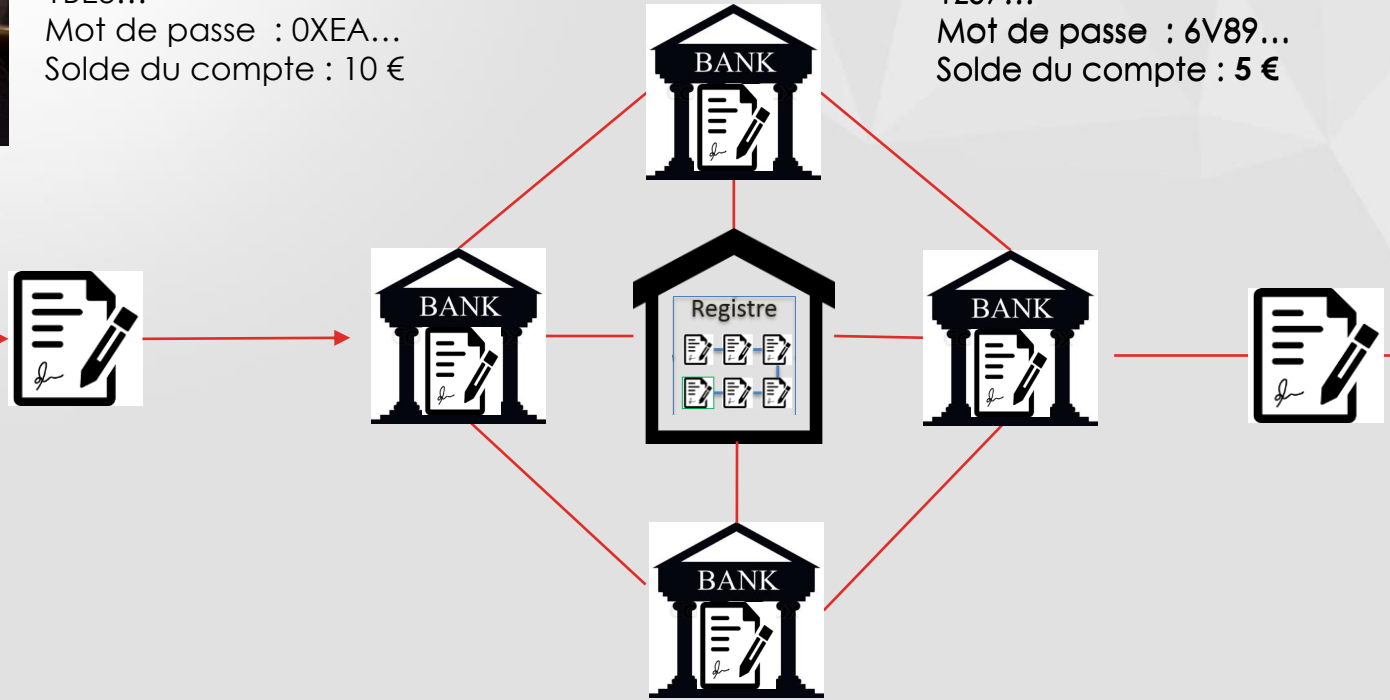


CARACTERISTIQUES DE LA TECHNOLOGIE BLOCKCHAIN

Réalisation d'une transaction dans le système traditionnel

Banque en ligne Bob
Numéro de compte (IBAN) :
1BE3…
Mot de passe : 0XEA…
Solde du compte : 10 €

Banque en ligne Alice
Numéro de compte (IBAN) :
1ZS7…
Mot de passe : 6V89…
Solde du compte : **5 €**



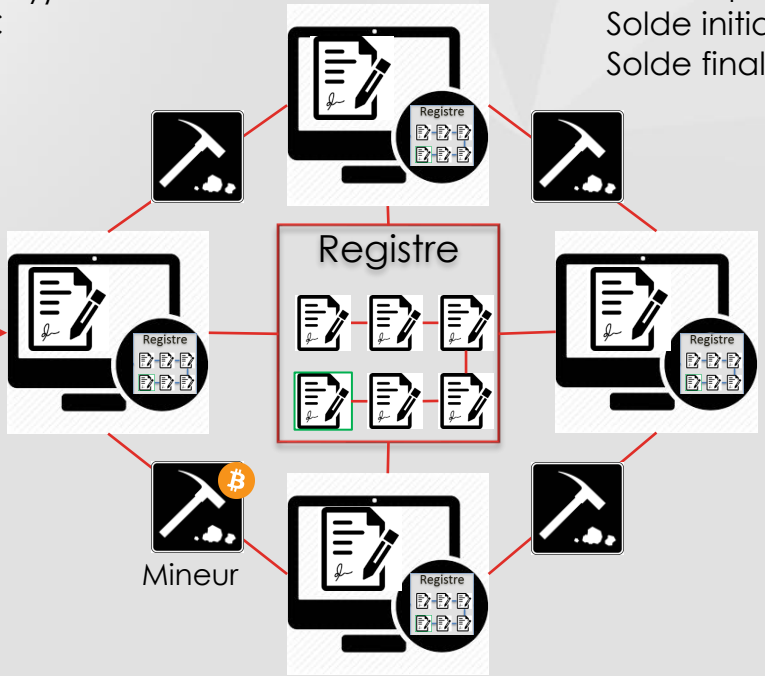
CARACTERISTIQUES DE LA TECHNOLOGIE BLOCKCHAIN

Réalisation d'une transaction bitcoin

Portefeuille Bob :
Public address (PubKey): 1BE3…
Mot de passe (PrivKey) : 0XEA…
Solde initial : 10 BTC
Solde final : 5 BTC

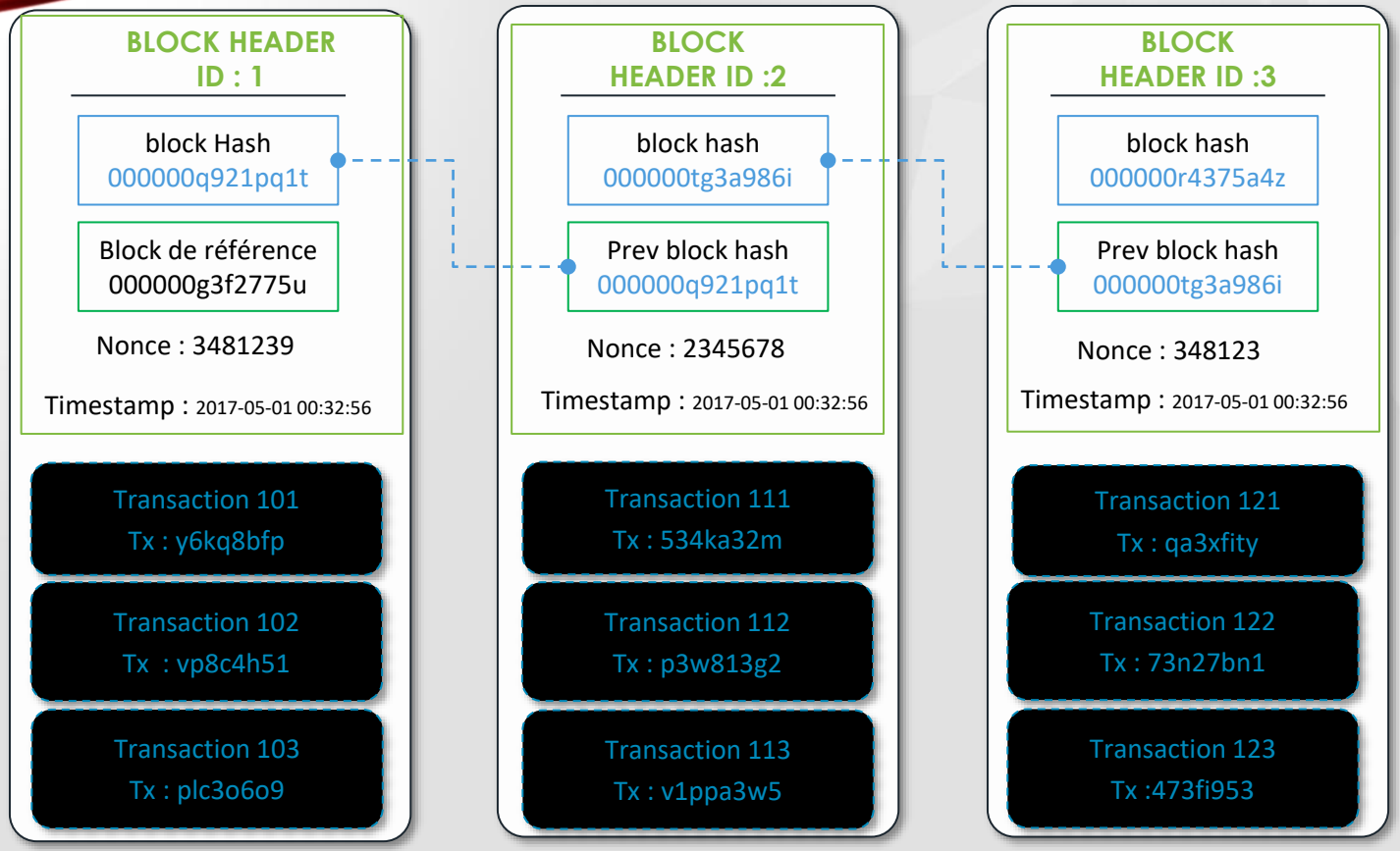
Portefeuille Alice :
Public address (PubKey): 1ZS7…
Mot de passe (PrivKey) : 6V89…
Solde initial : 0 BTC
Solde finale : 5 BTC

Bob transaction :
Destination Alice Pubkey 1ZS7 :
Montant : 5 BTC
Source Bob Pubkey 1B3E
Signature Bob (PrivKey)
Horodaté : 17-05-2017



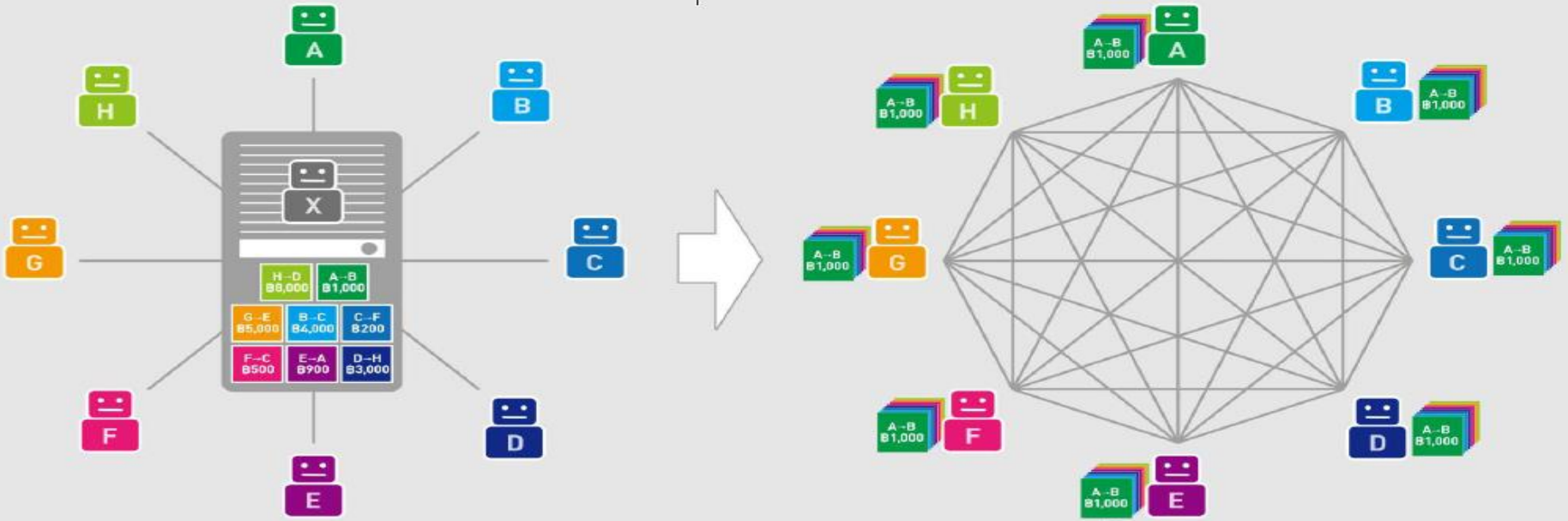
CARACTERISTIQUES DE LA TECHNOLOGIE BLOCKCHAIN

Le chainage des transactions sous forme de Block : Blockchain

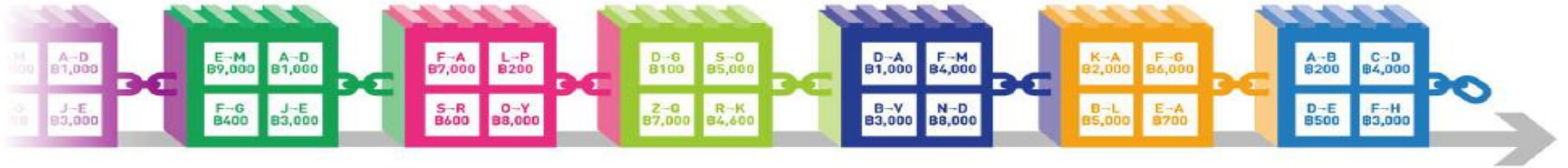


CARACTERISTIQUES DE LA TECHNOLOGIE BLOCKCHAIN

Registre distribué



BLOCKCHAIN : Transactions enregistrées dans des blocks qui sont ensuite validés et ajoutés à la chaine de blocks existante. Difficile à falsifier car les blocks sont liés par un processus cryptographique.



Les principaux avantages apportés :

- ✓ Pseudo anonyme : attribution d'un couple de clés (public / privé)
- ✓ Fongible : limitation du nombre maximum de tokens à 21 millions
- ✓ Immuable : Irréversibilité des transactions
- ✓ Auditable : Registre partagé par l'ensemble du réseau
- ✓ Authenticité : Chaque transaction est unique et horodatée
- ✓ Sécurisé : Utilisation de la cryptographie pour signer et valider toute transaction

La force de la communauté :

1. Les contributeurs :
   - Les développeurs : (https://github.com/bitcoin)
   - Les nœuds : (https://coin.dance/nodes)
   - Les mineurs : (https://blockchain.info/fr/pools)
   - La fondation Bitcoin (https://bitcoinfoundation.org/)
   - Les fournisseurs de services (wallet, plateforme de change etc…)

2. Les utilisateurs et enthousiastes (https://bitcoin.org/en/community)

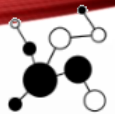
Qu'est ce qu'une cryptodevise ?

- Unité ou Jeton de transaction ayant une caractéristique fiduciaire et fongible au sein d'un système distribué de type Blockchain (Bitcoin, Ethereum …)

Quel est le rôle de la cryptodevise dans un système Blockchain ?

- Transférer un actif fongible/non fongible d'un point A vers un point B
- Rémunérer le mineur pour l'intégration de chaque transaction dans le Bloc « Transaction fees »
- Récompenser le mineur pour la conception d'un Bloc de transaction « Block reward »

CARACTERISTIQUES DE LA TECHNOLOGIE BLOCKCHAIN
La désintermédiation des données



Décentralisé

» Deux parties peuvent échanger sans crainte sans l'intervention d'un tiers de confiance
» Le risque de contrepartie est éliminé

INTÈGRE

» Toutes les transactions et écritures sont exécutées selon un protocole unique
» Les données sont horodatées, exhaustives, cohérentes, précises et disponibles

IMMUABLE

» Toutes les transactions et écritures sur une Blockchain sont immuables
» Les données ne peuvent pas être supprimées ou altérées

RAPIDE

» Les transactions et écritures sont réalisées en quelques minutes et traitées en permanence

ROBUSTE

» La décentralisation du réseau implique l'absence d'un point central de défaillance
» Le réseau est protégé des attaques courantes « DDoS, Sybil attack »

TRANSPARENT & CONFIDENTIEL

» Les données d'une Blockchain sont consultables par toutes les personnes qui y ont accès
» Les informations sont protégées par un processus de cryptage indéchiffrable

STANDARDISÉ

» Toutes les transactions sont portées par un registre unique et commun
» Le risque d'erreur lié au rapprochement de plusieurs registres est éliminé

ECONOMIQUE

» En éliminant les intermédiaires et tiers de confiance, un réseau Blockchain permet des économies substantielles sur les frais de transaction

CARACTERISTIQUES DE LA TECHNOLOGIE BLOCKCHAIN

La désintermédiation des données